Centre **risque & performance**

ÉCOLE POLYTECHNIQUE MONTRÉAL

Bulletin d'information **mars – avril 2007 Vol. 5 No. 2**

Lecture suggérée

Seeds of Disaster, Roots of Response : How Private Action Can Reduce Public Vulnerability

Comme le titre le laisse entendre, la principale thèse défendue dans cet ouvrage collectif veut que les actions prises par le secteur privé puissent contribuer à diminuer (ou augmenter) la vulnérabilité publique. La principale innovation de ce livre est le développement de la théorie des externalités sécuritaires (security externalities). Empruntée au secteur environnemental (externalités environnementales), cette théorie vient expliquer comment certains agents économiques privés sont réticents à engager des dépenses ayant pour objet d'augmenter leur robustesse face aux risques divers. Une externalité sécuritaire s'illustre par l'impact social d'une décision privée. Ces externalités peuvent tout aussi bien être positives que négatives. À titre d'exemple, une externalité sécuritaire négative peut s'illustrer par le scénario où une entreprise de distribution électrique décide d'acquérir un seul transformateur très puissant. Au niveau corporatif, cette décision est optimale en ce qu'elle permet une économie d'échelle tout en maintenant l'offre de service. Cependant, en cas de défaillance, l'absence de redondance entre les équipements et la diminution de la résilience du système vient augmenter la vulnérabilité des utilisateurs. Le défi en matière de politiques publiques est de mettre en œuvre un système d'incitatifs qui amènerait les agents économiques privés à prendre en compte les externalités sécuritaires dans leurs calculs de coûts optimaux.

Nous pouvons identifier, dans l'ouvrage étudié, deux grandes catégories de solutions. Premièrement, certains auteurs proposent des systèmes d'incitatifs fondés sur l'industrie de l'assurance. Il s'agirait d'utiliser les primes d'assurance pour récompenser les organisations investissant des ressources suffisantes en matière de protection de leurs infrastructures. De l'aveu même de plusieurs auteurs, peu de preuves empiriques viennent appuyer cette proposition. Des recherches plus poussées seront donc nécessaires pour en vérifier la pertinence.

Certains auteurs abordent ensuite la notion de confiance. Cette confiance ne peut être construite que par une collaboration intersectorielle saine et répondant aux besoins et contraintes de tous. Plusieurs modèles de collaboration sont proposés, allant de la collaboration transnationale à la collaboration avec les autorités locales. Le partage d'informations représente le défi le plus important.

Pour des raisons de concurrence sur le marché et de confidentialité des données de leurs clientèles, certaines organisations privées sont réticentes à fournir de l'information à leurs interlocuteurs publics. Inversement, pour des raisons de sécurité nationale, les gouvernements peuvent retenir certaines informations qui pourraient s'avérer pertinentes pour la sécurité de certaines entreprises privées. Pour surmonter ces obstacles, certains modèles sont proposés dont, par exemple, les tables de concertation sectorielles où les discussions ont lieu avec des secteurs spécifiques individuels (électricité, transport, télécoms, etc.). Il s'agit du modèle américain des *Information sharing and analysis centers* (ISACs).

(suite) Le problème avec ce modèle repose sur le fait que la collaboration entre secteurs spécifiques rend difficile la prise en compte de la problématique des interdépendances entre réseaux.

Les auteurs s'entendent tous pour affirmer que la collaboration est un outil pertinent pour éviter la réglementation et la contrainte. Si les organisations privées doivent faire certains sacrifices, les gouvernements le doivent aussi.

L'ouvrage, en général, est excellent et réunit des auteurs reconnus dans le domaine. La principale faiblesse, pour le lecteur canadien, découle des exemples exclusivement américains et, contexte oblige, il semble que le seul risque qui existe désormais est celui du terrorisme international ! Un tel ouvrage, avec des exemples de politiques de différents pays et préconisant une approche « tous-risques », deviendrait une référence incontournable.

Olivier Quenneville, étudiant à la maîtrise et associé de recherche, CRP

Référence : Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, Erwann O. Michel-Kerjan (dir.), Seeds of Disaster, Roots of Response : How Private Action Can Reduce Public Vulnerability, Cambridge, Cambridge University Press, 2006, 554 p.

Nouvelles brèves du CRP

Prochain séminaire du CRP / ASCQ

Les technologies de l'information en temps de crise : du télétravail au BlackBerry – des solutions de continuité opérationnelle?

Toute entreprise cherche à assurer sa continuité opérationnelle en temps de crise. Les technologies de l'information (TI) sont souvent les premiers outils vers lesquels se tournent les gestionnaires de mesures d'urgence. Mais sont-ils tous viables pour l'ensemble des entreprises ? Ont-elles les moyens techniques et financiers pour soutenir le télétravail sur une longue période de temps ? En terme de sécurité, quels sont les risques des TI ? Plus globalement, connaît-on les facteurs qui viendront affecter la demande en service sur le réseau IP des télécoms en situation de pandémie ?

Date : **vendredi 27 avril 2007**
Lieu : **École Polytechnique de Montréal**
Pavillon Lassonde, Local M-1010
Conférenciers : **Denis Bordeleau, Bell Canada**
Michel Renaud, Industrie Canada
Information : **irene.cloutier@polymtl.ca ou 514-340-4711 p.5927**

2e symposium du Programme conjoint de recherche sur les interdépendances entre les infrastructures (PCRII)

Le 6 mars prochain, le directeur du CRP, Benoît Robert, présentera les travaux du Centre aux représentants du ministère de la Sécurité publique et Protection civile Canada (SPPCC) et du Conseil de recherches en sciences naturelles et en génie (CRSNG). Les cinq autres équipes financées par le PCRII présenteront aussi l'avancé de leurs travaux. Un bilan complet sera préparé pour le prochain bulletin. http://www.psepc-sppcc.gc.ca/prg/em/jiirp/index-fr.asp.

Ce bulletin est publié par le *Centre risque & performance* de l'École Polytechnique de Montréal. Si vous désirez que votre nom soit ajouté ou retiré de la liste d'envoi, communiquez avec Irène Cloutier, tél. : 514-340-4711 poste 5927, courriel : irene.cloutier@polymtl.ca.

Les partenaires du *Centre risque & performance* : *Bell Canada, GazMétro, Hydro Québec (Production, Transport, Distribution), ministère de la Sécurité publique du Québec, ministère des Transports du Québec, ministère de la Sécurité publique et Protection civile Canada, Tecsult, Ville de Montréal (Centre de sécurité civile, Réseau d'aqueduc et d'égouts, Traitement de l'eau potable), Ville de Québec (Bureau de la sécurité civile).*